PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328117
(43)Date of publication of application : 30.11.1999

(51)Int.Cl. G06F 15/00
G06F 13/00
G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : 10-131491
(22)Date of filing : 14.05.1998

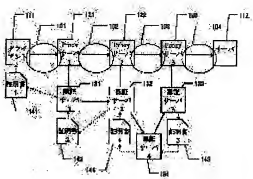
(71)Applicant : HITACHI LTD
(72)Inventor : MURAKAMI HIROMASA

(54) USER MANAGING METHOD OF AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the system which eliminates the need to register user information on a client to an authentication server that all proxy servers repeating signals between the client and a server belong to.

SOLUTION: Only the authentication server 131 which is closest to a client 111 registers the user and for subsequent authentication, certificates are handed over between authentication servers. When the client 111 connects to a server 112, authentication is done between the client 111 and the authentication server which is closest to it and then authentication is performed between authentication servers to hand over the certificate of the client 111; when the certificate reaches the authentication server that the proxy server 123 closest to the server 112 belongs to, route information is sent to the client. The client 111 performs authentication with the proxy server according to the route information to establish a connection up to the server 112 to the end.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－328117

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ
	13/00	３５１		13/00	３５１Ｚ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ
		６６０			６６０Ｅ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－131491

(22)出願日　平成10年(1998)５月14日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　村上　弘真
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

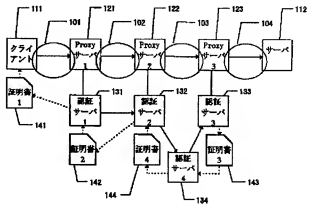
(74)代理人　弁理士　矢島　保夫

(54)【発明の名称】　認証システムにおけるユーザ管理方法

(57)【要約】　（修正有）

【課題】クライアントとサーバの間を中継する全てのプロキシサーバの属する認証サーバへクライアントのユーザ情報を登録する必要がない方式を提供する。

【解決手段】ユーザ登録をクライアントに最も近い認証サーバのみにし、それ以降の認証には認証サーバ間で証明書を受け渡すようにする。クライアントからサーバに接続する際には、クライアントとそれに最も近い認証サーバとの間で認証を行なった後、認証サーバ間で認証を行なってクライアントの証明書を受け渡していき、サーバに最も近いプロキシサーバが属する認証サーバまで辿り着いたら、経路情報をクライアントに送る。クライアントは、経路情報にしたがってプロキシサーバとの間で認証を行ない、最終的にサーバまでの接続を確立する。



【特許請求の範囲】
【請求項１】ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、
あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくとともに、
あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくことを特徴とする認証システムにおけるユーザ管理方法。
【請求項２】ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、
あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくステップと、
あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくステップと、
前記クライアントから前記サーバに接続するとき、前記クライアントから該クライアントに最も近い認証サーバに接続して認証を行なうステップと、
前記クライアントに最も近い認証サーバから、次に中継するプロキシサーバの属する認証サーバへ、接続し、認証サーバ間で受け渡した証明書を用いて認証サーバ間の認証を行なうとともに、前記クライアントの証明書を受け渡し、これを要求受付先のサーバに最も近いプロキシサーバの属する認証サーバに辿り着くまで繰り返すことにより、前記クライアントからサーバへ接続する際に中継するプロキシサーバの経路情報を取得するステップと、
中継するプロキシサーバの経路情報を前記クライアントに送るステップと、
前記経路情報に基づいて、前記クライアントと前記プロキシサーバとの間の認証を行なっていくことにより、前記クライアントと前記サーバ間の接続を確立するステップとを備えたことを特徴とする認証システムにおけるユーザ管理方法。
【請求項３】前記中継するプロキシサーバを、階層化した認証サーバで管理することを特徴とする請求項１または２の何れか１つに記載の認証システムにおけるユーザ管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、仮想プライベートネットワーク（Virtual Private NetWork：ＶＰＮ）に必要な認証を秘密鍵暗号方式を用いて実行するために用いるユーザ情報の管理作業、およびＶＰＮにおいてクライアントからサーバへ到達するために中継するプロキシ（Proxy）サーバの設定管理作業を軽減する、管理方法に関する。
【０００２】
【従来の技術】近年、インタネットから社内イントラネットへアクセスする等、公衆回線を使って安価にネットワークシステムを構築するニーズが高まっている。インタネットを介して、あたかも一つの企業内ネットワークに見せるシームレスな接続を提供するのがＶＰＮである。ＶＰＮでは、なりすましを防ぐためにユーザ認証を行ってからデータの送受信を開始し、また盗聴や改竄から公衆回線を流れるデータを守るために暗号化する機能を持つ。
【０００３】ＶＰＮの構成要素は、要求元のクライアント、要求受付先のサーバ、該クライアントおよびサーバ間の公衆回線上を流れるデータを暗号化／復号するプロキシサーバ、および、認証要求を受けてユーザの認証とユーザ管理を行う認証サーバに大別される。
【０００４】従来の秘密鍵暗号方式による認証では、例えば特開平０９－０６９８３１号「暗号通信システム」に示されるように、クライアントからプロキシサーバに接続すると、プロキシサーバの属する認証サーバが持つユーザ情報と、認証サーバからクライアントに配布した証明書とを元にして、認証が行われる。そのため、クライアントとサーバとの間で複数のプロキシサーバを中継する場合、全てのプロキシサーバの属する認証サーバから事前にクライアントへ証明書が配布されていなければいけない。
【０００５】また、要求元のクライアントから目的の要求受付先のサーバに接続するために、どのプロキシサーバを中継しなければいけないかを、事前に全てのプロキシサーバへ定義しておかなければいけなかった。
【０００６】
【発明が解決しようとする課題】上記従来技術では、要求元のクライアントと要求受付先のサーバの間を中継する全てのプロキシサーバの属する認証サーバへ、当該クライアントのユーザを登録しなければいけないことになる。多数のユーザが利用する、複数のプロキシサーバが存在するネットワーク環境では、ユーザの管理だけで多大な作業が必要になり、それぞれの認証サーバから発行された証明書を、発行先のユーザへ配布しなければいけない問題があった。また、要求元のクライアントから要求受付先のサーバまでの経路を事前に全てのプロキシサーバへ定義しておかなければならず面倒であった。
【０００７】本発明は、上述の従来技術における問題点に鑑み、クライアントとサーバの間を中継する全てのプ

ロキシサーバの属する認証サーバへ当該クライアントのユーザのユーザ情報を登録する必要がなく、また経路を事前に全てのプロキシサーバへ定義しておく必要もないような認証システムにおけるユーザ管理方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、請求項１に係る発明は、ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくとともに、あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくことを特徴とする。

【０００９】請求項２に係る発明は、ネットワーク接続されたクライアントとサーバとの間に置かれた複数のプロキシサーバと、クライアントとプロキシサーバとの間の認証を管理する認証サーバとを備えた認証システムにおけるユーザ管理方法であって、あらかじめ、前記クライアントから前記プロキシサーバを介して前記サーバにアクセスするユーザについて、前記クライアントに最も近い認証サーバに登録し、該認証サーバから証明書の配布を受けておくステップと、あらかじめ、認証サーバ同士で認証を行なうための証明書を、所定の認証サーバ間で受け渡しておくステップと、前記クライアントから前記サーバに接続するとき、前記クライアントから該クライアントに最も近い認証サーバに接続して認証を行なうステップと、前記クライアントに最も近い認証サーバから、次に中継するプロキシサーバの属する認証サーバへ、接続し、認証サーバ間で受け渡した証明書を用いて認証サーバ間の認証を行なうとともに、前記クライアントの証明書を受け渡し、これを要求受付先のサーバに最も近いプロキシサーバの属する認証サーバに辿り着くまで繰り返すことにより、前記クライアントからサーバへ接続する際に中継するプロキシサーバの経路情報を取得するステップと、中継するプロキシサーバの経路情報を前記クライアントに送るステップと、前記経路情報に基づいて、前記クライアントと前記プロキシサーバとの間の認証を行なっていくことにより、前記クライアントと前記サーバ間の接続を確立するステップとを備えたことを特徴とする。

【００１０】請求項３に係る発明は、請求項１または２において、前記中継するプロキシサーバを、階層化した認証サーバで管理することを特徴とする。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

【００１２】本実施の形態では、証明書の発行（ユーザの登録）をクライアントに最も近い認証サーバのみにし、ユーザ情報の管理作業を軽減する。証明書を発行した認証サーバ以外の認証サーバとの認証は、クライアントに最も近い認証サーバから次に中継するプロキシサーバの属する認証サーバへ、クライアントの証明書を認証サーバ間で順次受け渡し、クライアントの認証に使用する。また、要求受付先のサーバに最も近いプロキシサーバの属する認証サーバにたどりついた時点で、中継するプロキシサーバの情報をクライアントへ送り、その情報を元にクライアントと各認証サーバ間の認証を行っていく。

【００１３】上記の方式を実現するため、本実施の形態では、認証サーバ間で認証を行い、証明書を受け渡す機能を持つ。また中継するプロキシサーバの定義と次に中継するプロキシサーバが属する認証サーバの定義を認証サーバに持たせ、中継するプロキシサーバの検索は認証サーバが行う。さらに認証サーバは階層構造を持たせることにより、次に中継するプロキシサーバが属する認証サーバの定義の管理作業を軽減させる。

【００１４】以下、本実施の形態を詳しく説明する。なお、本実施の形態は、クライアントからサーバへの接続に３台のプロキシサーバを中継し、それぞれのプロキシサーバが属する認証サーバが３台あり、認証サーバ２，３が属する上位の認証サーバ４が存在するシステムを例として説明する。

【００１５】図１は、本実施の形態のシステム構成図である。図１において、ネットワーク環境は、ネットワーク１，２，３，４（１０１，１０２，１０３，１０４）で独立したネットワークである。各プロキシサーバ（１２１，１２２，１２３）とそれの属する認証サーバ（１３１，１３２，１３３）は、同一ネットワーク内にある。

【００１６】次に、要求元であるクライアント（１１１）について説明する。クライアント（１１１）は、サーバ（１１２）に接続してデータを送受信する形態のアプリケーションが動作するクライアントである。ＶＰＮの設定として、サーバ（１１２）に接続するにはプロキシサーバ１（１２１）を中継するという情報のみがクライアント（１１１）にあらかじめ定義されており、認証サーバ１（１３１）から証明書（１４１）が配布済みである。クライアント（１１１）上のアプリケーションからサーバ（１１２）への接続要求があると、クライアント（１１１）はプロキシサーバ１（１２１）に接続して、認証サーバ１（１３１）との認証を行う。図５に、クライアントのＶＰＮとしての動作を示す。図５の手順については後に詳述する。

【００１７】次に、要求受付先であるサーバ（１１２）について説明する。サーバ（１１２）ではアプリケーション

ョンサーバが起動していて、クライアント（１１１）からの接続を待機している。

【００１８】次に、プロキシサーバ１～３（１２１～１２３）について説明する。クライアント（１１１）に最も近いのがプロキシサーバ１（１２１）であり、ネットワーク１（１０１）と２（１０２）とを中継し、クライアント（１１１）から最初に認証要求のあるプロキシサーバである。サーバ（１１２）に最も近いプロキシサーバがプロキシサーバ３（１２３）であり、ネットワーク３（１０３）と４（１０４）とを中継し、サーバ（１１２）と平文データの送受信を行う、中継の終端となるプロキシサーバである。プロキシサーバ２（１２２）は、ネットワーク２（１０２）と３（１０３）とを中継するプロキシサーバである。図６に、これらのプロキシサーバの動作を示す。図６の手順については後に詳述する。

【００１９】次に、認証サーバ１～４（１３１～１３４）について説明する。プロキシサーバ１（１２１），２（１２２），３（１２３）が属する認証サーバが、それぞれ認証サーバ１（１３１），２（１３２），３（１３３）となる。ここでは１台のプロキシサーバが１台の認証サーバに属する場合を例として説明するが、複数台のプロキシサーバが１台の認証サーバに属することも可能である。認証サーバ１（１３１）は独立した１台の認証サーバであるが、認証サーバ２（１３２），３（１３３）は認証サーバ４（１３４）が統括する認証サーバグループを形成している。認証サーバ４は、この認証サーバグループ内の認証サーバ２（１３２），３（１３３）を統括する。

【００２０】各認証サーバには、クライアント（１１１）からサーバ（１１２）に接続するために次に中継すべきプロキシサーバが属する認証サーバを定義した中継経路定義情報が登録されている。図２に、その中継経路定義情報を示す。図２に示すように、認証サーバ１（１３１）には、サーバ（１１２）への接続要求が来たとき、次に中継すべきプロキシサーバの情報を持っているのが認証サーバ２（１３２）であることを示す中継経路定義情報が登録されている。認証サーバ２（１３２）には、中継経路定義情報は登録されていない。認証サーバ３（１３３）には、サーバ（１１２）への接続要求が来たとき、次にサーバ（１１２）と直接データの送受信が可能であることを示すＥｎｄが登録されている。認証サーバ４（１３４）には、サーバ（１１２）への接続要求が来たとき、次に中継すべきプロキシサーバの情報を持っているのが認証サーバ３（１３３）であることを示す中継経路定義情報が登録されている。

【００２１】各認証サーバには、クライアント（１１１）からサーバ（１１２）に接続するために接続を中継するプロキシサーバ（各認証サーバが管理するプロキシサーバ）を示す定義情報が登録されている。図３に、その定義情報を示す。図３に示すように、認証サーバ１（１３１）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ１（１３１）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ１（１２１）であることを示す定義情報が登録されている。認証サーバ２（１３２）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ２（１３２）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ２（１２２）であることを示す定義情報が登録されている。認証サーバ３（１３３）には、サーバ（１１２）への接続要求が来たとき、この認証サーバ３（１３３）で管理され、その接続要求を中継するプロキシサーバが、プロキシサーバ３（１２３）であることを示す定義情報が登録されている。認証サーバ４（１３４）には、そのような定義情報は登録されていない。

【００２２】各認証サーバには、認証サーバのグループを構成する上位の認証サーバを定義する定義情報が登録されている。図４に、その定義情報を示す。図４に示すように、認証サーバ２（１３２）には、自認証サーバの上位の認証サーバとして認証サーバ４（１３４）が登録されている。認証サーバ３（１３３）には、自認証サーバの上位の認証サーバとして認証サーバ４（１３４）が登録されている。認証サーバ１（１３１）および４（１３４）には、上位の認証サーバが登録されていない。

【００２３】クライアント（１１１）からサーバ（１１２）への接続は、認証サーバ１（１３１）が持つ証明書（認証サーバ１（１３１）がクライアント（１１１）に発行した証明書１（１４１））を中継経路定義に従って次の認証サーバへと順次送り、各認証サーバは一時的に証明書を保管し、クライアント（１１１）との認証に用いる。認証サーバ間の認証に使用する証明書は、事前に認証を要求する相手から配布されている必要がある。この例では、認証サーバ１（１３１）はあらかじめ認証サーバ２（１３２）が発行した証明書２（１４２）の配布を受けており、認証サーバ２（１３２）はあらかじめ認証サーバ４（１３４）が発行した証明書４（１４４）の配布を受けており、認証サーバ３（１３３）はあらかじめ認証サーバ４（１３４）が発行した証明書３（１４３）の配布を受けているものとする。接続を中継する次の認証サーバが、透過でない独立した別のネットワークに存在する場合、認証はプロキシサーバを中継して行われる。図７、図８、および図９に、認証サーバの動作を示す。図７、図８、および図９の手順については、後に詳述する。

【００２４】上記の環境で、クライアント（１１１）からサーバ（１１２）に対して接続要求があるときの処理手順を、図５～図９のフローチャートを参照して説明する。

【００２５】クライアント（１１１）からサーバ（１１２）に対して接続要求があると、クライアント（１１１）では図５の処理を開始する。まず、サーバ（１１

２）へ接続するのに中継するプロキシサーバを検索し（ステップ５０１）、当該プロキシサーバへ接続する（ステップ５０２）。クライアント（１１１）は、サーバ（１１２）に接続するためには、プロキシサーバ１（１２１）を中継すべきことを知っているので、ＶＰＮはプロキシサーバ１（１２１）へ接続し、認証を開始する（ステップ５０３）。すなわち、ステップ５０３で、プロキシサーバ１（１２１）へ、証明書１（１４１）を付けてクライアント（１１１）の認証要求を送信する。

【００２６】プロキシサーバ１（１２１）は、図６の処理で接続待ち状態になっているので、クライアント（１１１）からの証明書１（１４１）付きの認証要求を受信し（ステップ６０１）、プロキシサーバ１（１２１）が属する認証サーバ１（１３１）へ接続し（ステップ６０２）、クライアント（１１１）の認証要求を証明書１（１４１）を付けて送信する（ステップ６０３）。

【００２７】認証サーバ１（１３１）は、図７の処理で接続待ち状態になっているので、プロキシサーバ１（１２１）からのクライアント認証要求を受信し（ステップ７０１）、証明書１（１４１）と認証サーバ１（１３１）が管理するユーザ情報と比較して認証を行う（ステップ７０２）。認証に失敗したときは、コネクションを切断して（ステップ７０４）、接続待ちに戻る。認証に成功したときは、認証要求元を判定し（ステップ７０３）、認証要求元がクライアントからのときは、図８のステップ８０１に進み、認証要求元が認証サーバからのときは、図９のステップ９０１に進む。いまはクライアント（１１１）からの認証要求であるので、図８の処理を実行する。

【００２８】まず、証明書の種別を判別する（ステップ８０１）。クライアント（１１１）から送られてきた証明書１（１４１）は、いま処理を行なっている認証サーバ自らが発行したものであるから、ステップ８０２に進む。そして、次の認証サーバの情報を中継経路定義情報（図２）から検索する（ステップ８０２）。図２から分かるように、認証サーバ１（１３１）には、接続先がサーバ（１１２）である接続要求が来たとき、次の認証サーバは認証サーバ２（１３２）である旨が登録されている。そこで、検索結果として認証サーバ２（１３２）を得て、ステップ８０３からステップ８０５に進み、認証サーバ１（１３１）から認証サーバ２（１３２）へ接続し、証明書２を付けて認証サーバ２（１３２）に認証要求を送信する（ステップ８０５）。

【００２９】認証サーバ２（１３２）は、図７の処理で接続待ち状態になっているので、認証サーバ１（１３１）からの認証要求を受信し（ステップ７０１）、認証サーバ１（１３１）から送信された証明書２（１４２）と認証サーバ２（１３２）が管理する認証サーバ情報とを比較して認証を行う（ステップ７０２）。認証に失敗したときは、コネクションを切断して（ステップ７０４）、接続待ちに戻る。認証に成功したときは、認証要求元を判定する（ステップ７０３）。いまは認証要求元が認証サーバ１（１３１）からであるので、認証は成功し、図９の処理を実行することになる。

【００３０】認証サーバ２（１３２）における認証に成功したので、認証サーバ１（１３１）における処理は、ステップ８０５からステップ８０６を経て、ステップ８０８に進む。ここでクライアント（１１１）の証明書１（１４１）を、次の認証サーバである認証サーバ２（１３２）に送信し（ステップ８０８）、中継経路受信待ちに入る（ステップ８０９）。

【００３１】認証サーバ２（１３２）における図９の処理では、まず、クライアントの証明書１（１４１）を認証サーバ１（１３１）から受信して一時的に保存し（ステップ９０１）、次の認証サーバを中継経路定義情報（図２）から検索する（ステップ９０２）。検索した結果、認証サーバ２（１３２）には、サーバ（１１２）に対する次の認証サーバは登録されていないが、上位の認証サーバが定義（図４）されているため、ステップ９０３から９０４を経て、ステップ９０５に進み、認証サーバ４（１３４）へ接続し、証明書４を付けて認証サーバ４（１３４）に認証要求を送信する（ステップ９０５）。

【００３２】認証サーバ４（１３４）は、図７の処理で接続待ち状態になっているので、認証サーバ２（１３２）からの認証要求を受信し（ステップ７０１）、認証サーバ２（１３２）から送信された証明書４（１４４）と認証サーバ４（１３４）が管理する認証サーバ情報とを比較して認証を行う（ステップ７０２）。認証に失敗したときは、コネクションを切断して（ステップ７０４）、接続待ちに戻る。認証に成功したときは、認証要求元を判定する（ステップ７０３）。いまは認証要求元が認証サーバ２（１３２）からであるので、認証は成功し、図９の処理を実行することになる。

【００３３】認証サーバ４（１３４）における認証に成功したので、認証サーバ２（１３２）における処理は、ステップ９０５からステップ９０６を経て、ステップ９０８に進む。ここでクライアント（１１１）の証明書１（１４１）を、次の認証サーバである上位の認証サーバ４（１３４）に送信し（ステップ９０８）、中継経路受信待ちに入る（ステップ９０９）。

【００３４】認証サーバ４（１３４）における図９の処理では、まず、クライアントの証明書１（１４１）を認証サーバ２（１３２）から受信して一時的に保存し（ステップ９０１）、次の認証サーバを中継経路定義情報（図２）から検索する（ステップ９０２）。検索した結果、認証サーバ４（１３４）には、次の認証サーバは認証サーバ３（１３３）である旨が登録されている。そこで、ステップ９０３から９０５に進み、次の認証サーバ３（１３３）へ接続し、証明書３を付けて認証サーバ３

（１３３）に認証要求を送信する（ステップ９０５）。

【００３５】認証サーバ３（１３３）は、図７の処理で接続待ち状態になっているので、認証サーバ４（１３４）からの認証要求を受信し（ステップ７０１）、認証サーバ４（１３４）から送信された証明書３（１４３）と認証サーバ３（１３３）が管理する認証サーバ情報とを比較して認証を行う（ステップ７０２）。認証に失敗したときは、コネクションを切断して（ステップ７０４）、接続待ちに戻る。認証に成功したときは、認証要求元を判定する（ステップ７０３）。いまは認証要求元が認証サーバ４（１３４）からであるので、認証は成功し、図９の処理を実行することになる。

【００３６】認証サーバ３（１３３）における認証に成功したので、認証サーバ４（１３４）における処理は、ステップ９０５からステップ９０６を経て、ステップ９０８に進む。ここでクライアント（１１１）の証明書１（１４１）を、次の認証サーバである認証サーバ３（１３３）に送信し（ステップ９０８）、中継経路受信待ちに入る（ステップ９０９）。また、認証サーバ４（１３４）では、クライアント（１１１）の認証を行なわないため、証明書１（１４１）を一時保存しておく必要が無いから、証明書１は破棄する。

【００３７】認証サーバ３（１３３）における図９の処理では、まず、クライアントの証明書１（１４１）を認証サーバ４（１３４）から受信して一時的に保存し（ステップ９０１）、次の認証サーバを中継経路定義情報（図２）から検索する（ステップ９０２）。検索した結果、次の認証サーバは無く、Ｅｎｄが検出されるから、中継するプロキシサーバ３（１２３）の情報（図３）を認証サーバ４（１３４）へ中継経路情報として送信し（ステップ９１０）、コネクションを切断する。

【００３８】認証サーバ４（１３４）は、図９のステップ９０９で中継経路受信待ち状態にあるが、認証サーバ３（１３３）から送られてきた中継経路情報（サーバ（１１２）に接続するために最後に中継するプロキシサーバがプロキシサーバ３（１２３）であることを示す情報）を受信して（ステップ９０９）、該受信した中継経路情報を、認証要求元である認証サーバ２（１３２）へ送信し（ステップ９１０）、コネクションを切断する。なお、この認証サーバ４（１３４）におけるステップ９１０では、中継経路情報に何も付け加えない。図３から分かるように、認証サーバ４（１３４）には、中継するプロキシサーバの登録が無いからである。

【００３９】認証サーバ２（１３２）は、図９のステップ９０９で中継経路受信待ち状態にあるが、認証サーバ４（１３４）から送られてきた中継経路情報を受信して（ステップ９０９）、該受信した中継経路情報に、中継するプロキシサーバ２（１２２）の情報（図３）を付加して、認証要求元である認証サーバ１（１３１）へ送信し（ステップ９１０）、コネクションを切断する。結果として、認証サーバ１（１３１）に送られる中継経路情報は、「サーバ（１１２）に接続するためには、プロキシサーバ２，３の順に中継する」という情報になる。

【００４０】認証サーバ１（１３１）は、図８のステップ８０９で中継経路受信待ち状態にあるが、認証サーバ２（１３２）から送られてきた中継経路情報を受信して（ステップ８０９）、該受信した中継経路情報をプロキシサーバ１（１２１）へ送信し（ステップ８１０）、さらに認証成功を示す情報をプロキシサーバ１（１２１）へ送信する（ステップ８１１）。そして、ステップ７０４に進み、コネクションを切断する。

【００４１】プロキシサーバ１（１２１）は、認証サーバ１（１３１）から認証成功の通知を受信すると、ステップ６０４から６０５に進み、クライアント（１１１）に、認証の成功と共に、中継するプロキシサーバがプロキシサーバ２，３であることを通知する（ステップ６０５）。また、クライアント（１１１）から次の中継先であるプロキシサーバ２への接続要求を受信すると（ステップ６０７）、プロキシサーバ２へ接続して、データの中継を開始する（ステップ６０８）。

【００４２】クライアント（１１１）は、プロキシサーバ１（１２１）からの認証成功の通知を受信すると、ステップ５０４から５０５に進み、次に中継するプロキシサーバがプロキシサーバ２（１２２）であるから、プロキシサーバ１（１２１）を中継して、プロキシサーバ２（１２２）へ接続要求を送信し（ステップ５０６）、証明書１（１４１）を付けてプロキシサーバ２（１２２）へクライアントの認証要求を送信する（ステップ５０３）。

【００４３】プロキシサーバ１（１２１）は、ステップ６０８でデータを中継する状態にあるから、クライアント（１１１）からのプロキシサーバ２（１２２）への接続要求、および認証要求は、プロキシサーバ１（１２１）を経て、プロキシサーバ２（１２２）へ送れる。

【００４４】プロキシサーバ２（１２２）は、図６の処理で接続待ち状態になっているので、クライアント（１１１）からの証明書１（１４１）付きの認証要求を受信し（ステップ６０１）、プロキシサーバ２（１２２）が属する認証サーバ２（１３２）へ接続し（ステップ６０２）、クライアント（１１１）の認証要求を証明書１（１４１）を付けて送信する（ステップ６０３）。

【００４５】認証サーバ２（１３２）は、図７の処理で接続待ち状態になっているので、プロキシサーバ２（１２２）からのクライアント認証要求を受信し（ステップ７０１）、受信した証明書１（１４１）を用いて認証を行う（ステップ７０２）。認証サーバ２（１３２）では上述した処理により証明書１（１４１）が一時保存されているので認証は成功し、ステップ７０２から７０３に進む。また、認証要求元はクライアントであるので、図８の処理に進む（ステップ７０３）。図８において、証

明書種別の判定（ステップ８０１）では、受け取った証明書１（１４１）は認証サーバ２（１３２）が管理する証明書ではないため、中継経路定義の検索は行わず、認証が成功した時点でプロキシサーバ２（１２２）へ認証の成功を送信する（ステップ８１１）。認証終了後は、認証サーバ２（１３２）は証明書１（１４１）を破棄する。

【００４６】プロキシサーバ２（１２２）は、認証サーバ２（１３２）から認証成功の通知を受信すると、ステップ６０４から６０５に進み、クライアント（１１１）に、認証の成功を通知する（ステップ６０５）。また、クライアント（１１１）から次の中継先であるプロキシサーバ３への接続要求を受信すると（ステップ６０７）、プロキシサーバ３へ接続して、データの中継を開始する（ステップ６０８）。

【００４７】クライアント（１１１）は、プロキシサーバ２（１２２）からの認証成功の通知を受信すると、ステップ５０４から５０５に進み、次に中継するプロキシサーバがプロキシサーバ３（１２３）であるから、プロキシサーバ１（１２１），２（１２２）を中継して、プロキシサーバ３（１２３）へ接続要求を送信し（ステップ５０６）、証明書１（１４１）を付けてプロキシサーバ３（１２３）へクライアントの認証要求を送信する（ステップ５０３）。

【００４８】プロキシサーバ１（１２１），２（１２２）は、それぞれステップ６０８でデータを中継する状態にあるから、クライアント（１１１）からのプロキシサーバ３（１２３）への接続要求、および認証要求は、プロキシサーバ１（１２１），２（１２２）を経て、プロキシサーバ３（１２３）へ送られる。

【００４９】プロキシサーバ３（１２３）は、図６の処理で接続待ち状態になっているので、クライアント（１１１）からの証明書１（１４１）付きの認証要求を受信し（ステップ６０１）、プロキシサーバ３（１２３）が属する認証サーバ３（１３３）へ接続し（ステップ６０２）、クライアント（１１１）の認証要求を証明書１（１４１）を付けて送信する（ステップ６０３）。

【００５０】認証サーバ３（１３３）は、図７の処理で接続待ち状態になっているので、プロキシサーバ３（１２３）からのクライアント認証要求を受信し（ステップ７０１）、受信した証明書１（１４１）を用いて認証を行う（ステップ７０２）。認証サーバ３（１３３）では上述した処理により証明書１（１４１）が一時保存されているので認証は成功し、ステップ７０２から７０３に進む。また、認証要求元はクライアントであるので、図８の処理に進む（ステップ７０３）。図８において、証明書種別の判定（ステップ８０１）では、受け取った証明書１（１４１）は認証サーバ３（１３３）が管理する証明書ではないため、中継経路定義の検索は行わず、認証が成功した時点でプロキシサーバ３（１２３）へ認証の成功を送信する（ステップ８１１）。認証終了後は、認証サーバ３（１３３）は証明書１（１４１）を破棄する。

【００５１】プロキシサーバ３（１２３）は、認証サーバ３（１３３）から認証成功の通知を受信すると、ステップ６０４から６０５に進み、クライアント（１１１）に、認証の成功を通知する（ステップ６０５）。また、クライアント（１１１）から次の接続先であるサーバ（１１２）への接続要求を受信すると（ステップ６０７）、サーバ（１１２）へ接続して、データの中継を開始する（ステップ６０８）。

【００５２】クライアント（１１１）は、プロキシサーバ３（１２３）からの認証成功の通知を受信すると、ステップ５０４から５０５に進み、次に中継するプロキシサーバは無いから、サーバへの接続要求を送信する（ステップ５０７）。このときプロキシサーバ１（１２１），２（１２２），３（１２３）は、何れもステップ６０８でデータを中継する状態にある。クライアント（１１１）は、サーバ（１１２）との通信を開始する（ステップ５０８）。通信が終了したら（ステップ５０９）、コネクションを切断する（ステップ５１０）。これにより、各プロキシサーバのコネクションも次々に切断される（ステップ６０９）。

【００５３】クライアントの認証や、認証サーバ間の認証が失敗した場合は、失敗した時点で順次コネクションを切断し、クライアントアプリケーションにサーバへの接続失敗を通知する。

【００５４】

【発明の効果】以上説明したように、本発明によれば、全ての中継するプロキシサーバが属する認証サーバから証明書を事前に配布しておく必要がなく、ユーザの管理が容易にできる。また、認証サーバを階層化して認証サーバグループを形成することにより、認証サーバグループの中で最初に認証要求を受信する下位の認証サーバ全てに設定しなければいけない中継経路を、上位の１台の認証サーバで管理することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すシステム構成図。

【図２】各認証サーバに定義する、接続先サーバに対して次に中継するプロキシサーバの情報を持っている認証サーバを定義する説明図。

【図３】各認証サーバに定義する、接続先サーバへの接続を中継するプロキシサーバを定義する説明図。

【図４】各認証サーバに定義する、認証サーバのグループを構成するために上位の認証サーバを定義する説明図。

【図５】クライアントのＶＰＮとしての動作を示すフローチャート図。

【図６】プロキシサーバの動作を示すフローチャート図。

【図７】認証サーバの動作を示すメインフローチャート図。

【図８】認証サーバがクライアントとの認証処理を示すサブフローチャート図。

【図９】認証サーバが認証サーバ間の認証処理を示すサブフローチャート図。

【符号の説明】

１０１，１０２，１０３，１０４…それぞれ独立した（透過でない）ネットワーク１，２，３，４。

１１１…クライアントアプリケーションが動作する計算機。

１１２…サーバアプリケーションが動作してクライアントからの接続を待機する計算機。

１２１，１２２，１２３…ネットワーク間を中継する計算機。

１３１，１３２，１３３，１３４…クライアントのユーザ認証と認証サーバ間の認証を行う計算機。

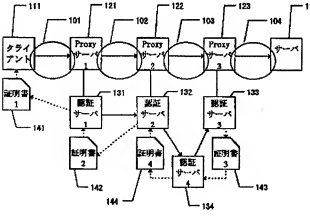
１４１…認証サーバ１からクライアントへ配布した証明書。

１４２…認証サーバ２から認証サーバ１へ配布した証明書。

１４３…認証サーバ３から認証サーバ４へ配布した証明書。

１４４…認証サーバ４から認証サーバ２へ配布した証明書。

【図１】



【図２】

認証サーバ	接続先	次の認証サーバ
認証サーバ１(131)	サーバ(112)	認証サーバ２(132)
認証サーバ２(132)	－	－
認証サーバ３(133)	サーバ(112)	Ｅｎｄ
認証サーバ４(134)	サーバ(112)	認証サーバ３(133)

（注）Ｅｎｄ：サーバと直接データの送受信が可能

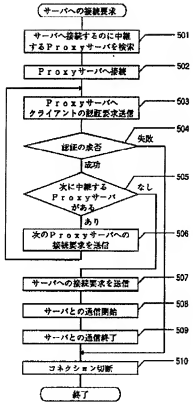
【図３】

認証サーバ	接続先	中継するＰｒｏｘｙサーバ
認証サーバ１(131)	サーバ(112)	Ｐｒｏｘｙサーバ１(121)
認証サーバ２(132)	サーバ(112)	Ｐｒｏｘｙサーバ２(122)
認証サーバ３(133)	サーバ(112)	Ｐｒｏｘｙサーバ３(123)
認証サーバ４(134)	－	－

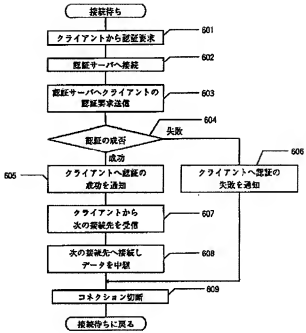
【図４】

認証サーバ	上位の認証サーバ
認証サーバ１(131)	－
認証サーバ２(132)	認証サーバ４(134)
認証サーバ３(133)	認証サーバ４(134)
認証サーバ４(134)	－

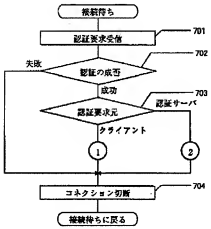
【図５】


サーバへの接続要求
サーバへ接続するのに中継するＰｒｏｘｙサーバを検索
501
Ｐｒｏｘｙサーバへ接続
502
Ｐｒｏｘｙサーバへクライアントの認証要求送信
503
認証の成否
失敗
504
成功
次に中継するＰｒｏｘｙサーバがあるか
なし
505
あり
次のＰｒｏｘｙサーバへの接続要求を送信
506
サーバへの接続要求を送信
507
サーバとの通信開始
508
サーバとの通信終了
509
コネクション切断
510
終了

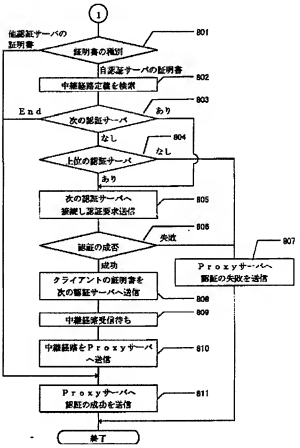
【図６】


接続待ち
クライアントから認証要求
501
認証サーバへ接続
502
認証サーバへクライアントの認証要求送信
503
認証の成否
失敗
604
成功
606
505
クライアントへ認証の成功を通知
クライアントへ認証の失敗を通知
クライアントから次の接続先を受信
607
次の接続先へ接続しデータを中継
608
コネクション切断
609
接続待ちに戻る

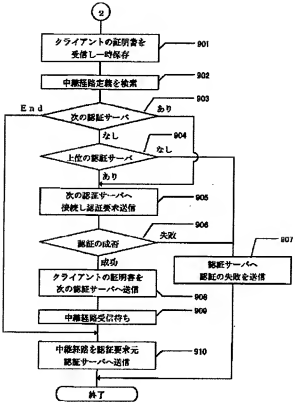
【図７】


接続待ち
認証要求受信
701
認証の成否
702
失敗
成功
認証要求元
認証サーバ
703
クライアント
1
2
コネクション切断
704
接続待ちに戻る

【図８】


1
他認証サーバの証明書
証明書の識別
801
自認証サーバの証明書
中継経路定義を検索
802
End
次の認証サーバ
803
あり
なし
804
なし
上位の認証サーバ
あり
次の認証サーバへ接続し認証要求送信
805
認証の成否
806
失敗
807
成功
Ｐｒｏｘｙサーバへ認証の失敗を通信
クライアントの証明書を次の認証サーバへ送信
808
中継経路受信待ち
809
中継経路をＰｒｏｘｙサーバへ送信
810
Ｐｒｏｘｙサーバへ認証の成功を送信
811
終了

【図９】


②
クライアントの証明書を受信し一時保存
901
中継経路定義を検索
902
903
次の認証サーバ
あり
End
なし
904
上位の認証サーバ
なし
あり
次の認証サーバへ
候補し認証要求送信
905
906
認証の成否
失敗
907
認証サーバへ
認証の失敗を送信
成功
クライアントの証明書を
次の認証サーバへ送信
908
909
中継経路受信待ち
910
中継経路を認証要求元
認証サーバへ送信
終了